BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT/FR 99/02692

RÉPUBLIQUE FRANÇAISE

09/831634

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

REC'D 22 NOV 1999
WIPO PCT

FR99/2692

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED BUT NOT IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 10 NOV. 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

cerfa N° 55-1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 12/11/97

N° D'ENREGISTREMENT NATIONAL

DÉPARTEMENT DE DÉPÔT 75 98 14224

DATE DE DÉPÔT 12 NOV. 1998

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT-SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

n°du pouvoir permanent | références du correspondant | téléphone

BM/014275 01.40.67.11.99

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ▷ demande initiale

☐ certificat d'utilité ☐ transformation d'une demande de brevet européen ▽ ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

PROCEDE D'AUTHENTIFICATION ENTRE UNE CARTE A MEMOIRE ET UN TERMINAL.

3 DEMANDEUR (S) n° SIREN 749711200 code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

GEMPLUS

Forme juridique

Société en Commandite par par Actions

Nationalité (s) Française

Adresse (s) complète (s) Pays

Avenue du Pic de Bertagne
Parc d'activités de la Plaine de Jouques
13420 GEMENOS

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(nom et qualité du signataire)

Paul BALLOT
92-1009
CABINET BALLOT SCHMIT

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL

9814224

~~BM/014275~~

TITRE DE L'INVENTION :

PROCEDE D'AUTHENTIFICATION ENTRE UNE CARTE A MEMOIRE ET UN TERMINAL.

LE(S) SOUSSIGNÉ(S)

Cabinet BALLOT SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

COOREMAN Pascal

domicilié (s) au :

Cabinet BALLOT SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Paris, le 10 novembre 1998

Paul BALLOT - 92-1009
Cabinet BALLOT SCHMIT

BA 113/140697

PROCEDE D'AUTHENTIFICATION ENTRE UNE CARTE A MEMOIRE ET UN TERMINAL

L'invention concerne les cartes à mémoire et les terminaux auxquels elles sont susceptibles d'être connectées de temps à autre et, plus particulièrement, un procédé qui permet à la carte à mémoire et au terminal de s'authentifier.

Les cartes à mémoire, du fait qu'elles ne comportent pas un microprocesseur, ne peuvent pas mettre en oeuvre un algorithme d'authentification qui implique des calculs. Cependant, certaines cartes à mémoire mettent en oeuvre un algorithme sous forme câblée qui permet l'authentification dite "active" de la carte par le terminal mais pas l'authentification inverse du terminal par la carte. Par suite de leur faible coût, les cartes à mémoire sont très utilisées dans de nombreuses applications telles que les cartes de fidélité, les contrôles d'accès, les paiements privatifs, etc ... . Cependant, par suite de l'absence d'authentification, leur sécurité d'emploi est vulnérable de sorte qu'on leur préfère parfois des cartes à microprocesseur pour certaines applications. Mais ces cartes à microprocesseur sont d'un coût nettement plus élevé, d'autant plus élevé que l'algorithme d'authentification est élaboré, ce qui conduit à les écarter pour des applications bon marché. Aussi, le but de la présente invention est d'obtenir la sécurité d'emploi des cartes à mémoire.

Ce but est atteint en mettant en oeuvre un procédé d'authentification dans lequel tous les calculs algorithmiques sont effectués par le terminal auquel la carte à mémoire est connectée.

Par ailleurs, les opérations relatives à l'authentification sont effectuées avant le début d'une transaction proprement dite et après la fin de cette transaction en vue de l'authentification au début de la transaction suivante.

L'invention concerne donc un procédé d'authentification entre une carte à mémoire comportant au moins un compteur et un terminal, caractérisé en ce qu'il comprend les étapes suivantes consistant à :

(a) Insérer la carte à mémoire dans le terminal,

(b) Calculer dans le terminal un code secret CSC_1 selon une fonction cryptographique F de plusieurs variables comprenant au moins un code CSN identifiant la carte à mémoire et la valeur dudit compteur,

(c) Authentifier le terminal par la carte lorsque le code secret calculé CSC_1 est identique à un code CSC_0 enregistré dans la mémoire à la fin de la précédente authentification selon l'opération (f) ci-après,

(d) exécuter la transaction prévue et modifier la valeur dudit compteur,

(e) calculer dans le terminal un nouveau code secret CSC_2 selon la fonction cryptographique F du code CSN identifiant la carte à mémoire et de la nouvelle valeur dudit compteur,

(f) mettre à jour la carte à mémoire pour la prochaine transaction en enregistrant dans la mémoire, le nouveau code secret CSC_2 calculé par l'opération (e).

Pour obtenir l'authentification de la carte par le terminal, le procédé comprend les étapes supplémentaires suivantes entre les étapes (c) et (d) consistant à :

(x) calculer dans le terminal un certificat d'authentification CA_1 selon une fonction cryptographique G de plusieurs variables comprenant au moins le code CSN identifiant la carte à mémoire et la valeur dudit compteur,

(y) authentifier la carte par le terminal lorsque le certificat d'authentification calculé CA_1 est identique à un certificat CA_0 calculé et enregistré dans la carte à la fin de la précédente transaction selon les étapes (e') et (f') ci-après :

- en ce que l'étape (e) est complétée par l'étape suivante consistant à :
  (e') calculer dans le terminal un nouveau certificat d'authentification CA_2 selon la fonction cryptographique G,
- et en ce que l'étape (f) est complétée par l'étape suivante consistant à :
  (f') mettre à jour la carte à mémoire pour la prochaine transaction en enregistrant dans la mémoire le nouveau certificat d'authentification CA_2 calculé selon l'étape (e').

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description suivante d'un exemple particulier de réalisation, ladite description étant faite en relation avec le dessin joint dans lequel :

- la figure 1 est un schéma simplifié d'une carte à mémoire, et
- la figure 2 est un diagramme montrant les opérations effectuées entre le terminal et la carte à mémoire lors d'une transaction.

Le procédé de l'invention s'applique (figure 1) à une carte à mémoire CM qui comprend bien entendu une mémoire M mais aussi un compteur CT dit de transactions qui compte les transactions effectuées entre la carte

CM et un terminal TE auquel la carte est connectée par insertion.

La carte à mémoire CM peut aussi comprendre un deuxième compteur CE dit d'authentification qui compte les demandes d'authentification, ces demandes d'authentification pouvant intervenir à tout moment lors d'une transaction et indépendamment de cette dernière.

Ces deux compteurs CE et CT peuvent faire partie de la mémoire M selon des dispositifs connus.

En outre, la mémoire M de la carte comprend une première zone à accès non protégé en lecture dans laquelle est enregistré, par exemple le numéro de série CSN de la carte dans une partie ZCSN, et une deuxième zone à accès protégé pour le reste de la mémoire, cette deuxième zone comportant des parties qui sont affectées à l'enregistrement de valeurs particulières telles qu'un Certificat d'Authentification CA dans la partie ZCA et une balance BAL et son certificat d'authentification CBAL dans la partie ZBAL.

Une troisième zone ZCSC est réservée à l'enregistrement d'un code secret CSC et son accès pour enregistrement est soumis à la présentation du code secret CSC.

La mémoire M est adressée par un circuit d'adressage ADR et la transmission bilatérale des signaux entre le terminal TE et la carte CM s'effectue par l'intermédiaire d'un circuit interface INT.

Par ailleurs, la carte comprend un comparateur CP qui compare le code CSC lu dans la partie ZCSC à un code fourni par le terminal TE, le résultat de la comparaison permettant ou non l'adressage de la zone protégée de la mémoire M.

Le procédé selon l'invention sera décrit dans le cadre d'une authentification mutuelle entre la carte et le terminal en mettant en oeuvre le seul compteur de

transactions CT et des fonctions cryptographiques dites à sens unique mais le procédé de l'invention peut également s'appliquer à la seule authentification du terminal par la carte, à la mise en oeuvre simultanée des deux compteurs CE et CT et de fonctions cryptographiques autres que celles à sens unique. Les différentes opérations, notamment cryptographiques, peuvent être réalisées soit dans le terminal TE, soit dans un module de sécurité, soit encore dans un dispositif distant.

De préférence, le procédé d'authentification mutuelle selon l'invention comprend les étapes suivantes consistant à :

(m) Insérer la carte CM dans le terminal TE, cette étape pouvant comporter la présentation d'un code personnel PIN de l'utilisateur de la carte,

(n) Calculer dans le terminal TE une clé de session Ks_1 en :

(n_1) lisant le numéro de série CSN de la carte CM,

(n_2) lisant le contenu CTC_1 du compteur de transactions CT de la carte CM et,

(n_3) calculant une clé de session Ks_1 selon une fonction cryptographique à sens unique F_{ks} telle que :

$Ks_1 = F_{ks}(K_m, CSN, CTC_1)$

- K_m étant une clé-mère enregistrée dans le terminal TE,
- F_{ks} étant par exemple une fonction du type hachage,

(o) Calculer, dans le terminal TE, un code secret CSC_1 de la carte à l'aide d'une fonction cryptographique F telle que :

$CSC_1 = F(Ks_1)$,

(p) Authentifier le terminal TE par la carte CM en :

(p_1) transmettant le code secret CSC_1 à la carte CM,

(p_2) comparant dans le comparateur CP ce code secret CSC_1 à un code secret CSC_0 enregistré dans la carte CM à la fin de la précédente transaction avec la carte, et

(p_3) autorisant la suite des opérations si la comparaison indique l'identité $CSC_0 = CSC_1$ ou en la refusant dans le cas contraire ;

(q) Calculer dans le terminal TE un Certificat d'Authentification CA_1 tel que :

$CA_1 = G(Ks_1)$

- G étant une fonction cryptographique, et

(r) Authentifier la carte CM par le terminal TE en :

(r_1) lisant le contenu CA_0 de la zone ZCA de la mémoire de la carte CM,

(r_2) transmettant au terminal TE le contenu CA_0 de cette zone protégée ZCA qui correspond à un Certificat d'Authentification CA_0 calculé à la fin de la précédente transaction,

(r_3) comparant dans le terminal TE le Certificat d'Authentification calculé CA_1 au certificat CA_0, et

(r_4) autorisant la suite des opérations si la comparaison indique l'identité $CA_1 = CA_0$;

(s) Exécuter la transaction, cette transaction pouvant consister par exemple à mettre à jour une zone de mémoire ZBAL indiquant l'état du crédit ou balance BAL restant dans la carte CM en :

(s_1) lisant dans la zone ZBAL la valeur BAL_0 de la balance résultant de la transaction précédente et le certificat correspondant $CBAL_0$,

(s_2) vérifiant que le certificat $CBAL_0$ correspond bien au résultat de la fonction cryptographique telle que :

$CBAL_0 = H\ (K_t, BAL_0, CSN, CTC_1)$,
- K_t étant une clé de transaction,
(s_3) incrémentant le compteur de transactions à la valeur $(CTC_1 + 1) = CTC_2$
(s_4) enregistrant la nouvelle balance BAL_1 dans la zone ZBAL,
(s_5) calculant un Certificat $CBAL_1$ de la nouvelle balance BAL_1 telle que :
$CBAL_1 = H(K_t, BAL_1, CSN, CTC_2)$, et
(s_6) enregistrant $CBAL_1$ dans la zone ZBAL ;

(t) Mettre à jour la carte CM pour la prochaine transaction avec un nouveau code secret CSC_2 et un nouveau certificat CA_2, en
(t_1) calculant dans le terminal TE :
- la future clé de session Ks_2 telle que :
$Ks_2 = F(K_m, CSN, CTC_2)$
- le futur code secret CSC_2 tel que :
$CSC_2 = F(Ks_2)$,
- le futur certificat d'authentification CA_2 tel que :
$CA_2 = G(Ks_2)$,
(t_2) enregistrant le code secret CSC_2 dans la mémoire M de la carte CM dans la zone protégée et le certificat d'authentification CA_2 dans la zone protégée ZCA.

L'invention a été décrite avec un exemple particulier de réalisation dans lequel la transaction est une opération sur la valeur balance de la carte ; cependant, l'invention s'applique à toute autre transaction selon les applications prévues pour la carte considérée.

Dans cet exemple particulier, la transaction se termine par une incrémentation du compteur de transactions CT à une valeur CTC_2 qui est égale habituellement à $(CTC_1 + 1)$. Cependant, cette valeur de CTC_2 peut être

différente de (CTC_1 + 1) et être égale, par exemple, à (CTC_1 + 3).

Ce compteur de transactions doit être incrémenté ou décrémenté à chaque transaction même si l'opération conduit à ne pas changer la balance ; dans ce cas, il faut effectuer la transaction en réenregistrant la balance inchangée mais le certificat $CBAL_1$ sera différent car le compteur de transactions aura été incrémenté. Il en sera de même du nouveau code secret CSC_2 et du certificat CA_2.

Les variables des fonctions F, G et F_{ks} qui ont été retenues dans l'exemple sont la clé-mère, le numéro de série CSN et la valeur CTC du compteur de transactions. Cependant, des variables additionnelles peuvent être utilisées telles que le code personnel PIN de l'utilisateur de la carte, ce code étant entré dans le terminal après insertion de la carte.

L'invention a été décrite dans le cadre d'une authentification mutuelle carte/terminal mais elle s'applique de manière plus générale d'abord à une authentification du terminal par la carte, cette première authentification pouvant être suivie ou non par une authentification de la carte par le terminal, l'ensemble des deux authentifications réalisant une authentification mutuelle.

L'exemple décrit utilise des fonctions cryptographiques F, G et F_{ks} utilisant des variables telles qu'une clé-mère K_m, une clé de session K_s et une clé de transaction K_t, mais de telles clés ne sont pas nécessaires pour mettre en oeuvre l'invention.

La valeur du compteur d'authentifications CE est de préférence utilisée pour le calcul du code secret CSN tandis que la valeur du compteur de transactions CT est de préférence utilisée pour le calcul du certificat d'authentification CA.

REVENDICATIONS

1. Procédé d'authentification entre une carte à mémoire (CM) comportant au moins un compteur (CE, CT) et un terminal (TE), caractérisé en ce qu'il comprend les étapes suivantes consistant à :

(a) Insérer la carte à mémoire (CM) dans le terminal (TE),

(b) Calculer dans le terminal un code secret CSC_1 selon une fonction cryptographique F de plusieurs variables comprenant au moins un code CSN identifiant la carte à mémoire et la valeur (CTE_1, CTC_1) dudit compteur (CE, CT),

(c) Authentifier le terminal par la carte lorsque le code secret calculé CSC_1 est identique à un code CSC_0 enregistré dans la mémoire à la fin de la précédente authentification selon l'opération (f) ci-après,

(d) exécuter la transaction prévue et modifier la valeur (CTE_2, CTC_2) dudit compteur (CE, CT),

(e) calculer dans le terminal (TE) un nouveau code secret CSC_2 selon la fonction cryptographique F du code CSN identifiant la carte à mémoire (CM) et de la nouvelle valeur (CTE_2, CTC_2) dudit compteur (CE, CT),

(f) mettre à jour la carte à mémoire (CM) pour la prochaine transaction en enregistrant dans la mémoire (M), le nouveau code secret CSC_2 calculé par l'opération (e).

2. Procédé selon la revendication 1, caractérisé :

- en ce qu'il comprend les étapes supplémentaires suivantes entre les étapes (c) et (d) consistant à :

(x) calculer dans le terminal (TE) un certificat d'authentification CA_1 selon une fonction cryptographique G de plusieurs variables comprenant au moins le code CSN identifiant la carte à mémoire et la valeur (CTE_1, CTC_1) du compteur (CE, CT),

(y) authentifier la carte (CM) par le terminal (TE) lorsque le certificat d'authentification calculé CA_1 est identique à un certificat CA_0 calculé et enregistré à la fin de la précédente transaction selon les étapes (e') et (f') ci-après :

- en ce que l'étape (e) est complétée par l'étape suivante consistant à :

(e') calculer dans le terminal (TE) un nouveau certificat d'authentification CA_2 selon la fonction cryptographique G du code CSN identifiant la carte à mémoire et de la nouvelle valeur (CTE_2, CTC_2) dudit compteur (CE, CT),

- et en ce que l'étape (f) est complétée par l'étape suivante consistant à :

(f') mettre à jour la carte à mémoire (CM) pour la prochaine transaction en enregistrant dans la mémoire (M) le nouveau certificat d'authentification CA_2 calculé selon l'étape (e').

3. Procédé selon la revendication 1, caractérisé :

- en ce que l'étape (b) consiste à :

- calculer d'abord dans le terminal (TE) une clé de session K_{s1} selon une fonction cryptographique F_{ks} de plusieurs variables comprenant au moins une clé-mère K_m connue du terminal (TE), le code CSN identifiant la carte à mémoire (CM) et la valeur (CTE_1, CTC_1) dudit compteur (CE, CT),

- calculer ensuite dans le terminal (TE) le code secret CSC_1 selon la fonction cryptographique F de la clé de session K_{s1},

- en ce que l'étape (e) consiste à :
  - calculer d'abord dans le terminal (TE) une nouvelle clé de session K_{s2} selon la fonction cryptographique F_{ks} avec la nouvelle valeur (CTE_2, CTC_2) dudit compteur (CE, CT),
  - calculer ensuite dans le terminal (TE) le nouveau code secret CSC_2 selon la fonction cryptographique F de la nouvelle clé de session K_{s2}.

4. Procédé selon la revendication 2 et 3, caractérisé en ce que :
- l'étape (e') consiste à calculer le nouveau certificat d'authentification CA_2 selon la fonction cryptographique G de la nouvelle clé de session K_{s2}.

5. Procédé selon l'une quelconque des revendications précédentes 1 à 4, dans son application à une carte à mémoire (CM) comprenant deux compteurs, l'un (CE) comptant les authentifications et l'autre (CT) comptant les transactions de paiement, caractérisé en ce que les variables des fonctions cryptographiques F, G et F_{ks} comprennent les valeurs (CTE_1, CTE_2, CTC_1, CTC_2) desdits compteurs.

6. Procédé selon l'une des revendications précédentes caractérisé en ce que les fonctions cryptographiques F, G et F_{ks} sont des fonctions à sens unique.

7. Procédé selon la revendication 6, caractérisé en ce que les fonctions cryptographiques F, G et F_{ks} sont des fonctions de "hachage".

8. Procédé selon l'une des revendications précédentes 3 à 7, caractérisé en ce que l'étape (b) comprend les étapes suivantes consistant à :

(b_1) lire le numéro de série CSN de la carte (CM),
(b_2) lire le contenu (CTE_1 et/ou CTC_1) du compteur, et
(b_3) calculer la clé de session selon une fonction cryptographique F_{ks} telle que :
$Ks_1 = F_{ks}(K_m, CSN, CTC_1)$.

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que l'étape (c) comprend les étapes suivantes consistant à :

(c_1) transmettre le code secret CSC_1 à la carte CM,
(c_2) comparer dans la carte ce code secret CSC_1 à un code secret CSC_0 enregistré dans la carte CM à la fin de la précédente transaction avec la carte, et
(c_3) autoriser la suite des opérations si la comparaison indique l'identité $CSC_0 = CSC_1$ ou en la refusant dans le cas contraire.

10. Procédé selon l'une des revendications 2 à 9, caractérisé en ce que l'étape (y) comprend les étapes suivantes consistant à :

(y_1) lire le contenu CA_0 de la zone ZCA de la mémoire de la carte CM,
(y_2) transmettre au terminal (TE) le contenu CA_0 de cette zone ZCA qui correspond à un Certificat d'Authentification CA_0 calculé à la fin de la précédente transaction,
(y_3) comparer dans le terminal TE le Certificat d'Authentification calculé CA_1 au certificat CA_0, et
(y_4) autoriser la suite des opérations si la comparaison indique l'identité $CA_1 = CA_0$.

11. Procédé selon l'une des revendications 1 à 10, caractérisé en ce que l'étape (d) comprend, dans le cas d'une modification de la balance BAL_0, les étapes suivantes consistant à :

(d_1) lire dans une zone ZBAL de la mémoire (M) la valeur BAL_0 de la balance résultant de la transaction précédente et le certificat correspondant $CBAL_0$, et

(d_2) vérifier que le certificat $CBAL_0$ correspond bien au résultat de la fonction cryptographique telle que :

$CBAL_0 = H (K_t, BAL_0, CSN, CTC_1)$,

- K_t étant une clé de transaction,

(d_3) incrémenter le compteur de transactions à la valeur $(CTC_1 + 1) = CTC_2$

(d_4) enregistrer la nouvelle balance BAL_1 dans la zone ZBAL,

(d_5) calculer un Certificat $CBAL_1$ de la nouvelle balance BAL_1 telle que :

$CBAL_1 = H(K_t, BAL_1, CSN, CTC_2)$, et

(d_6) enregistrer $CBAL_1$ dans la zone ZBAL.

12. Procédé selon l'une des revendications précédentes 1 à 11, caractérisé en ce que :

- l'étape (a) comprend en outre une étape d'entrée du code personnel PIN de l'utilisateur.

13. Procédé selon l'une des revendications précédentes 3 à 12, caractérisé en ce que :

- dans l'étape (b), l'une des variables utilisées pour le calcul de session Ks_1 est le code personnel PIN de l'utilisateur.

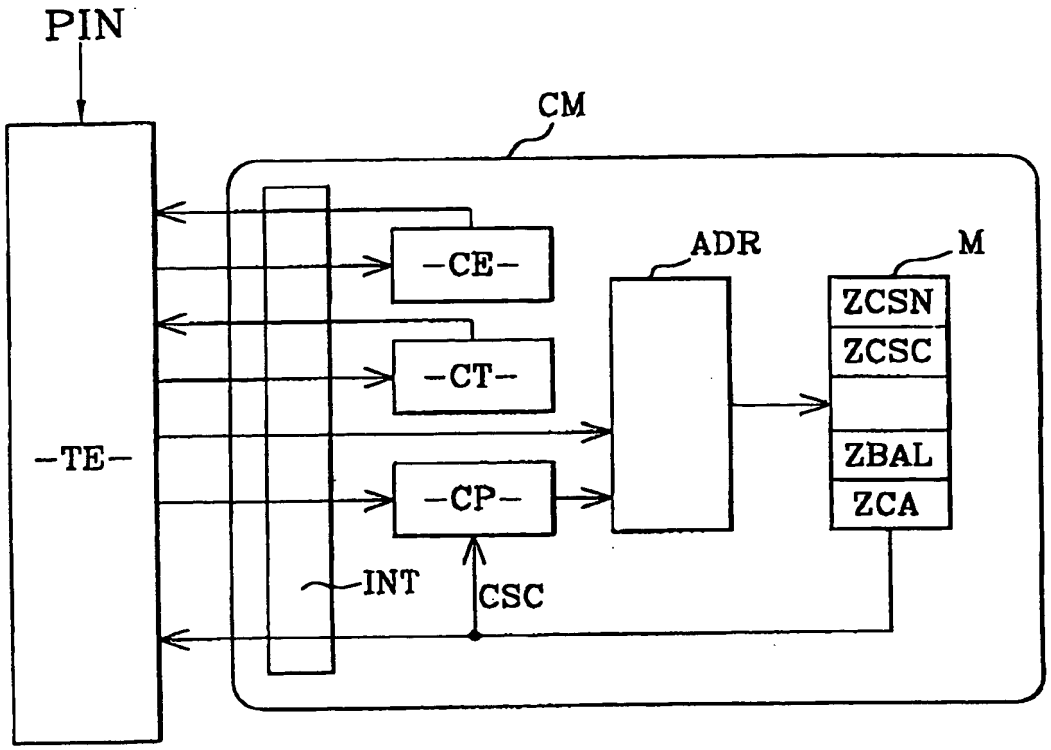

FIG.1

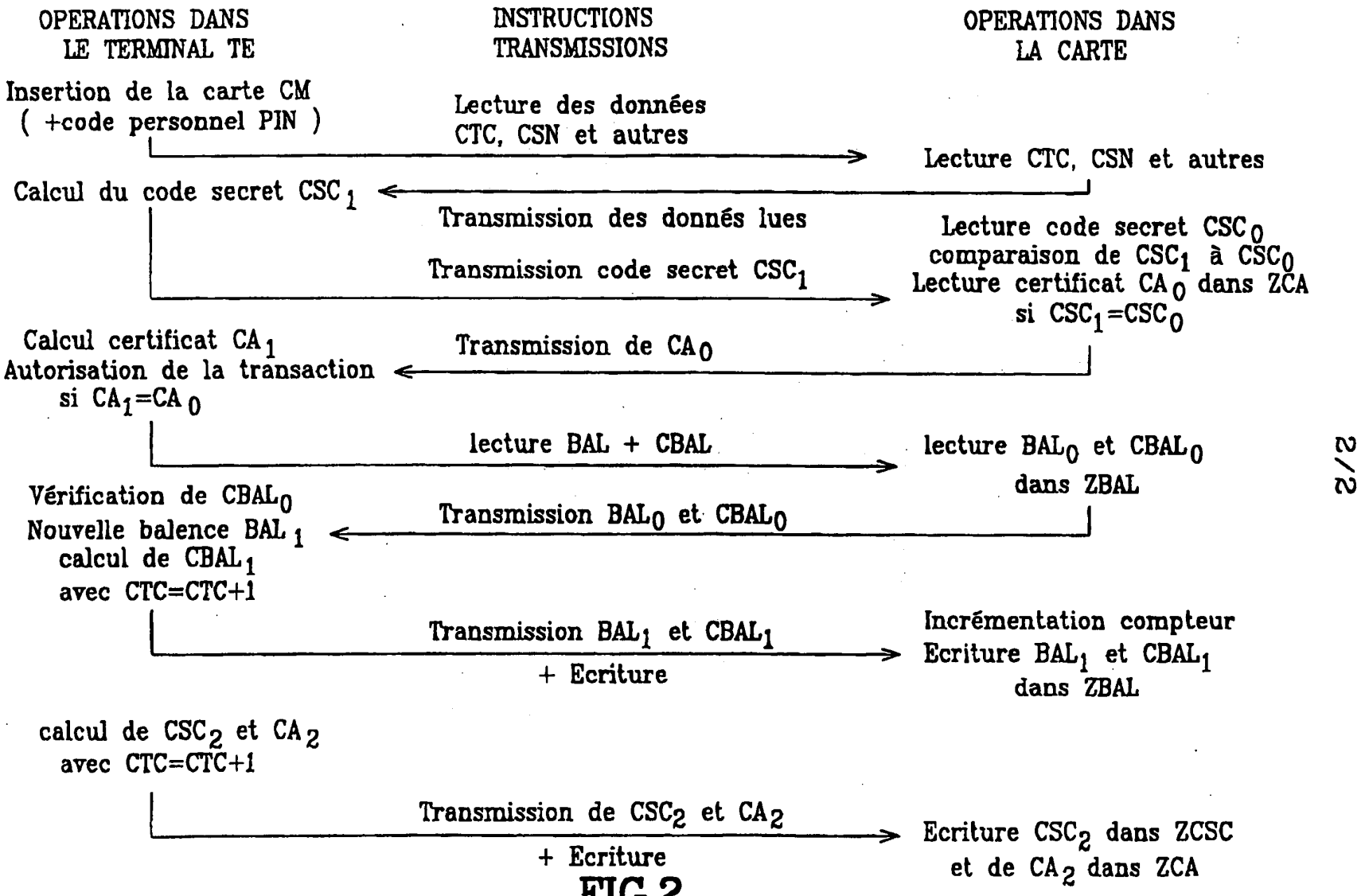
OPERATIONS DANS LE TERMINAL TE
INSTRUCTIONS TRANSMISSIONS
OPERATIONS DANS LA CARTE
Insertion de la carte CM (+code personnel PIN)
Lecture des données CTC, CSN et autres
Lecture CTC, CSN et autres
Calcul du code secret CSC1
Transmission des donnés lues
Lecture code secret CSC0
comparaison de CSC1 à CSC0
Transmission code secret CSC1
Lecture certificat CA0 dans ZCA
si CSC1=CSC0
Calcul certificat CA1
Autorisation de la transaction
si CA1=CA0
Transmission de CA0
lecture BAL + CBAL
lecture BAL0 et CBAL0
dans ZBAL
Vérification de CBAL0
Nouvelle balence BAL1
calcul de CBAL1
avec CTC=CTC+1
Transmission BAL0 et CBAL0
Transmission BAL1 et CBAL1
+ Ecriture
Incrémentation compteur
Ecriture BAL1 et CBAL1
dans ZBAL
calcul de CSC2 et CA2
avec CTC=CTC+1
Transmission de CSC2 et CA2
+ Ecriture
Ecriture CSC2 dans ZCSC
et de CA2 dans ZCA

FIG.2